DOI:10.13530/j.cnki.jlis.185006

欧盟数据保护影响评估制度及其启示*

肖冬梅　谭礼格

摘　要　欧盟数据保护影响评估制度起源于隐私影响评估制度,数据保护影响评估制度的实施主体是数据控制者,规制对象是具有高风险的数据处理行为,具体流程包括审查、咨询、评估、报告和保障及复审五个阶段。欧盟数据保护影响评估制度对数据保护有风险防控作用,企业可因此更被消费者信赖。数据保护影响评估制度有指导性规范与行业自律结合、强制性义务两种模式。欧盟数据保护影响评估制度对于我国个人信息和重要数据安全风险评估制度配套法规的制定和落地,尤其是在安全风险评估的适用范围、评估性质、流程设计与机构设置等方面,具有重要的借鉴意义。图3。表1。参考文献19。

关键词　数据保护影响评估　隐私影响评估　欧盟

分类号　G203

EU Data Protection Impact Assessment and Its Implications

XIAO Dongmei & TAN Lige

ABSTRACT

The research on the European Union's Data Protection Impact Assessment (DPIA) is to detect how EU addresses data security risks in the era of big data through a sophisticated assessment system. DPIA, originated from Privacy Impact Assessment (PIA), is contained in the PIA. The main differences of them lie in the scope, nature and time of generation.

The implementing subject of DPIA is the data controller. The data controller, as the decision maker and implementer, plays the core role in the whole process of DPIA. Its main tasks are to identify the need to implement DPIA, organize the DPIA group, consult the Data Protection Officer(DPO) under stipulated circumstances, seek the views of data subjects or their representatives on the measures after implementing a DPIA, and consult data supervisory authority beforehand when the risk is high.

The regulated object of DPIA is the data processing which will result in a high risk to the rights and freedoms of natural persons. Adopting a new technology is often risky; as a result, GDPR sets this as the general statutory situation of high risks. In addition, GDPR lists three special situations of high risks, i.e., automatic, systematic processing and evaluation of personal information, large-scale processing of sensitive data and large-scale monitoring of publicly accessible area.

* 本文系国家社会科学基金重点项目"云环境下数字学术信息资源安全的法律保障体系研究"(编号:14AZD076)的研究成果之一。(This article is an outcome of the project "Research on the Legal Guarantee System of Digital Academic Information Resources Security Under Cloud Environment" (No. 14AZD076) supported by National Social Science Foundation of China.)

通信作者:肖冬梅,Email:86650210@qq.com,ORCID:0000-0001-7611-2058(Correspondence should be addressed to XIAO Dongmei, Email:86650210@qq.com,ORCID:0000-0001-7611-2058)

A DPIA involves five stages: examination, consultation, assessment, report, safeguard and review. The examination is to conduct a preliminary analysis of the data processing behavior involved to identify the need to perform a DPIA. The consultation is interspersed in the various periods of review, assessment, report and safeguard. Based on the basic information obtained during the examination, the assessment determines the protection objectives, identifies the potential attackers, the motives of the attackers, and the types of attack outcomes through the simulation exercise of the project or plan, and then the assessment criteria will be identified.

The risk level of the project or plan will be determined according to the criteria, and the results of the assessment must be audited by a neutral and objective organization. After the assessment, the data controller needs to create and publish a DPIA report in a special format; it has four response modes of control, acceptance, termination and transfer for different levels of assessment, which can be used separately or combined. The review is that, after the report is completed, the data controller should verify whether the data processing has taken corresponding safeguard measures according to the assessment results when necessary. And the purpose of the review is to monitor continuously.

The EU DPIA strengthens the prevention and control of data risks by establishing data controllers' obligations and sophisticated process. On one hand, such arrangements of the system will help relevant companies to save costs and to gain consumers' trust and market reputation. On the other hand, it is beneficial for data subjects to realize the control and protection of their own data. From the evolution path and development of modes of the EU PIA to DPIA, China has two alternatives in the legislative mode in the case of data protection impact assessment. The first is to actively promote industry self-discipline on the basis of national guidance. The second is to set the data protection impact assessment as mandatory requirement. The EU DPIA can act as a meaningful reference to the formulation and enforcement of Chinese laws and regulations on security risk assessment system for personal information and important data, especially to the scope of application, nature of assessment, design of process and mechanism of security risk assessment. 3 figs. 1 tab. 19 refs.

KEY WORDS

Data protection impact assessment.　Privacy impact assessment.　European Union.

0　引言

随着信息技术的快速发展与广泛应用,人类社会日益步入数据化社会。欧盟 1995 年通过的《关于涉及个人数据处理的个人保护以及此类数据自由流通和第 95/46/EC/号指令》(*EU Data Protection Directive* 95/46/*EC*,以下简称《95 指令》)已难以适应数据技术带来的社会变革,也不能有效地保护数据主体的基本权利,建立统一数字化市场的目标为制定欧盟内统一的适用法提供了契机[1]。为此,自 2009 年 5 月起,欧盟委员会展开对《95 指令》修改的公开讨论,2012 年 1 月 25 日,欧盟委员会出台了替代《95 指令》的欧盟《统一数据保护条例》(*General Data Protection Regulation*,以下简称 GDPR)(草案),经过 4 年多的讨论和多次修改,2016 年 4 月 14 日,GDPR 经欧盟委员会投票通过,并于 2018 年 5 月 25 日生效。GDPR 强化了数据主体的各项权利,同时对义务主体提出了更严格的要求,加重了后者的数据保护义务和责任。GDPR 中增加的诸多义务如数据保护影响评估、

事先咨询与事先授权、向数据主体通知数据泄漏、向监管机构上报数据泄漏等,而其中最能够防范风险、监测风险的是数据保护影响评估(Data Protection Impact Assessment,简称 DPIA)。DPIA 与其说是一项义务,不如说是一种制度,其系统性与全面性对我国建立个人信息和重要数据安全风险评估制度有一定启示与借鉴意义。本文试图通过追溯 DPIA 的起源和演进,透析 DPIA 制度的基本内容、运行方式、影响和模式选择,为我国个人信息安全影响评估制度的出台提供有益借鉴和参考。

1 DPIA 制度溯源

DPIA 制度是欧盟对隐私影响评估制度(Privacy Impact Assessment,PIA)进行转用和继承的产物,故要了解 DPIA 制度必先解析 PIA 制度。

1.1 PIA 制度的缘起

PIA 制度起源于 20 世纪 90 年代,起因是信息技术的发展导致虚拟交流增多、面对面交谈减少,隐私风险剧增。对 PIA 制度没有统一的定义,大致有从方法论、工具和过程、评估结果影响以及生命周期几个角度所进行的阐释[2]。2011 年 1 月 12 日,欧盟出台了一个针对 RFID(无线射频识别技术)的 PIA 制度框架文件,其将 PIA 制度定义为一个工具:通过设计系统化程序评估特定 RFID 应用对隐私和数据保护产生的影响,并采取适当的行动以防止或使这些影响最小化的工具[3]。Wright 将其定义为一种方法:评估项目、政策、方案、服务、产品或其他活动的隐私影响,与利益相关者协商并采取必要的补救行动,以避免或减少负面影响[4]。概而言之,PIA 制度是一项对技术或行为的隐私影响进行评估,并采取适当的措施以防止或使这些影响最小化的制度。

1.2 PIA 制度的基本内容

英国是欧洲最早实施 PIA 制度的国家,于 2007 年由信息专员办公室发布 PIA 制度手册,2009 年修订;紧随其后的爱尔兰于 2010 年发布 PIA 制度指南。放眼全球,PIA 制度在各国的发展先后和应用范围不一,总的来说,PIA 在澳大利亚、加拿大、爱尔兰、新西兰和英国的应用最为广泛[5],但基本内容大同小异。PIA 制度分为全面(Full-Scale)PIA 制度和局部(Small-Scale)PIA 制度。全面 PIA 制度包括五个阶段:①初步审查阶段,审查项目计划的内容和背景;②准备阶段,分析利益相关者后组建 PIA 制度咨询小组、准备咨询策略;③咨询与分析阶段,咨询利益相关者并分析、修改项目文件和隐私设计文件,并登记所有文件;④记录阶段,登记所有文件的最终版本并制定 PIA 制度报告。此阶段的重要目的之一是形成公司记忆库,即使当初参与的员工已经离开,也能确保项目经验可以反复适用;⑤回顾与审计阶段,再次检查隐私设计文件中的策略并做回顾报告。局部 PIA 制度简化了以上步骤和内容,针对的是如门禁卡、数据库更新、更换条形码等相对较小而具体的问题,但当其涉及高度敏感的个人数据或所涉技术未经检查时,则可能会转换成全面 PIA 制度。判断适用全面 PIA 制度还是局部 PIA 制度,需要有一个由不同层次的不同问题构成的筛选工具,这个筛选工具包括 4 个层次的问题:①有必要实施全面 PIA 制度吗?该层次包含 11 个问题,如果回答都是“否”则进入下一层次;②有必要实施局部 PIA 制度吗?该层次包含 15 个测试,如果多个测试的答案是肯定的,则转入全面 PIA 制度,如果所有的回答是否定的则进入下一层次;③有必要实施隐私法合规审查吗?该层次包含 3 个问题,如果有任何一个回答是肯定的,则需实施;④有必要实施数据保护法合规审查吗?该层次包含 2 个问题,通过这两个问题确定公司是否有遵守数据保护法[6]。

1.3 DPIA 制度与 PIA 制度的对比

DPIA 和 PIA 是包含与被包含的关系,主要

的差别体现在三个方面:一是范围不一致[7]。PIA 制度针对个人隐私的影响,DPIA 制度关注个人数据保护的影响,这两种影响是有区别的。根据情报价值链理论,数据是接近事实的最小单位,是一切事物的最基本单元,数据比隐私范围大。二是性质不同。DPIA 制度已经上升为一项法定义务,具有法定性、强制性。PIA 制度虽对少数国家的政府机关来说是一项强制性义务,例如美国、英国和加拿大,但在大多数国家主要还是作为一种风险防控的商业手段,多体现在行业制度、企业内部规范之中。三是产生的时间有别,隐私影响评估制度在前,已有十余年的发展史,而数据保护影响评估制度是在 2018 年 5 月实施的 GDPR 中才正式确立。

2　DPIA 制度的基本内容

DPIA 制度源自《95 指令》。根据《95 指令》第 19 条第 1 款第 6 项规定,数据控制者或其代表向监管机构报告的内容,包括对数据控制者所采取措施是否适当的初步评估的总体说明,而其措施是否适当,主要看其是否按《95 指令》第 17 条规定,采取了能确保数据处理安全的措施;《95 指令》第 20 条规定,成员国应明确可能给数据主体的权利和自由带来特殊风险的数据处理行为,并在实施之前对其进行检查。《统一数据保护条例(GDPR)2012 年建议案》(以下简称《12 草案》)第 33 条新增 DPIA 义务,并最终被纳入 GDPR 第 35 条。DPIA 制度体现了数据最小化原则(即控制数据处理行为应限制在所必需的最少数量内)[8]和数据质量原则(即个人数据的处理需合目的性和准确性)[9]。

根据 GDPR 第 35 条第 1 款的规定,DPIA 是指运用新技术处理数据时,考虑到该数据处理的本质、范围和目的,可能给自然人的权利和自由带来的高风险,数据控制者应当在数据处理之前评估该数据处理计划可能给个人数据保护带来的影响。评估结果可以适用于一系列具有相同高风险的类似数据处理行为[10]。按照法理学分类,DPIA 是一项强制性义务,只需要满足特定条件,即在数据处理会给自然人的权利和自由带来高风险时,数据控制者应当进行数据保护影响评估;按照审查机制的分类,DPIA 制度是事前审查和事后监督的结合,具有预先性、主动性和全面性。GDPR 第 35 条对于高风险的界定并未采取下定义的方式,而是采用了列举法,在该条第 3 款中罗列了三类具有高风险的典型场景,例如:数据处理涉及数据画像、敏感数据、与刑事定罪和犯罪有关的个人数据及大规模的公开监测等。除此之外,该条第 2 款规定,在实施评估时,数据控制者应当咨询指定数据保护官的义务;第 4 款和第 5 款规定了监管机构建立数据处理行为清单的义务;第 6 款规定了适用一致性机制的情形;第 7 款规定了评估的内容;第 8 款规定了考虑相关行为准则以判断评估的目的;第 9 款规定了在进行评估时咨询数据主体或其代表人的义务;第 10 款规定了一种实施评估的例外情形,即当数据处理有相关法律依据时,一般情况下,评估可不再进行,但成员国认为必须进行的除外;第 11 款则规定了评估以后的复审义务。

2.1　DPIA 制度的实施主体

根据 GDPR 第 4 条第 7 款,数据控制者指单独或与他人共同确定个人数据处理的目的和方式的自然人、法人、公共权力机关、代理机构或其他机构;个人数据处理的目的和方式应由欧盟或成员国法律决定,数据控制者或其任命的具体标准也可由欧盟或成员国法律规定。数据控制者在 DPIA 制度的整个流程中发挥核心作用,是 DPIA 制度运行的决策者和实施者。数据控制者的主要任务是决定是否实施 DPIA,组建 DPIA 小组,指定情形下咨询数据保护官,就 DPIA 的处理咨询数据主体或其代表人,高风险时事先咨询数据保护监管机构以及复审。

2.2 DPIA 制度的规制对象

DPIA 制度的规制对象是对自然人的权利和自由会产生高风险的数据处理行为。根据 GDPR 第 4 条第 2 款的规定,数据处理行为可分为对内和对外两种,区分的关键在于有无数据控制者、数据处理者和数据主体之外的第三方主体出现。对内数据处理行为是指,无论是否为通过自动化方式对个人数据进行的处理,只要是在内部(多用于内网或无网络状态下)进行的数据操作,都属于对内数据处理行为,包括数据收集、记录、组织、建构、存储、修改、恢复、查询、使用等。对外数据处理行为是指通过传播、分发方式对外进行披露,或者获得、组合、限制、清除或销毁个人数据的行为,多用于互联网状态下。运用新技术时往往会产生风险,故 GDPR 第 35 条第 1 款将运用新技术作为"高风险"的一般法定情形。此外,第 3 款列举了三种具有高风险的特殊情形(见图 1):自动化系统处理和评估个人信息,基于评估所做的决策会对相关自然人产生法律效力或类似的显著影响时,包括数据画像(Profiling);当大规模地处理特殊数据时,例如生物数据;当对公开访问区域的大规模系统监测时,例如 CCTV[11]。

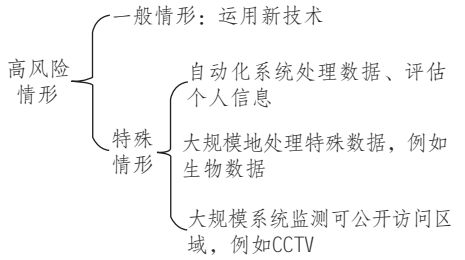

图 1 高风险情形

3 DPIA 流程

按照 GDPR 相关规定的字面理解,DPIA 在程序上大致是:数据处理操作—识别高风险—咨询数据保护官、数据主体或其代表人—制作数据处理操作清单—事后复审(见图 2)。

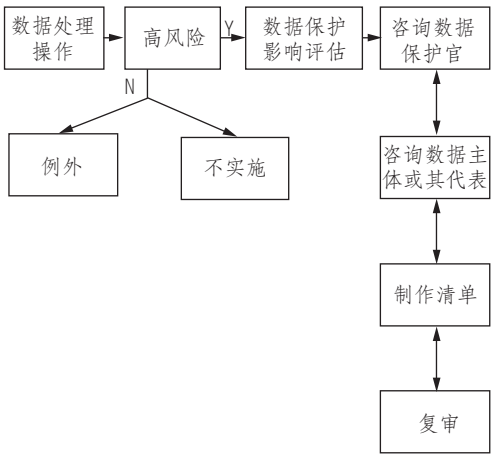

图 2 DPIA 的程序

Bieker, Friedewald, Hansen 等学者将 DPIA 分为准备阶段、评估阶段以及报告和保护三个阶段。数据控制者在准备阶段需要决定是否需要实施 DPIA,在评估阶段识别保护目标和潜在威胁、设立评估基准并实施风险评估,在报告和保护阶段识别并实施合适的保障措施、采用标准格式书面记录评估结果、形成并公布 DPIA 报告、审计评估结果[12]。对 DPIA 流程进行这样的阶段划分,虽然有助于更好地理解该制度,但是这样的划分忽视了两个重要环节:一是咨询,二是复审。《欧盟基本权利宪章》(*Charter of Fundamental Rights of the European Union*)第 41 条规定,在作出任何对他人有不利影响的措施之前,需要听取他人的意见,就像在刑事审判中要保护被告的最后陈述权一般,这就意味着咨询利益相关者这一环节在整个 DPIA 流程中至关重要。再者,复审程序是 GDPR 特别增设的一个环节,旨在通过再次审查确保实施 DPIA 后确定的保护措施都已到位,避免 DPIA 的实施流于形式。将咨询和复审这两个程序单独划分成一个阶段更有利于理解 DPIA 流程的内在连贯性,对 DPIA 流程的细分也有助于阐述该制度的系统性。故在三阶段的基础上可将 DPIA 细分成审查、咨询、评估、报告与保障以及复审五阶段(DPIA 流程见图 3)。

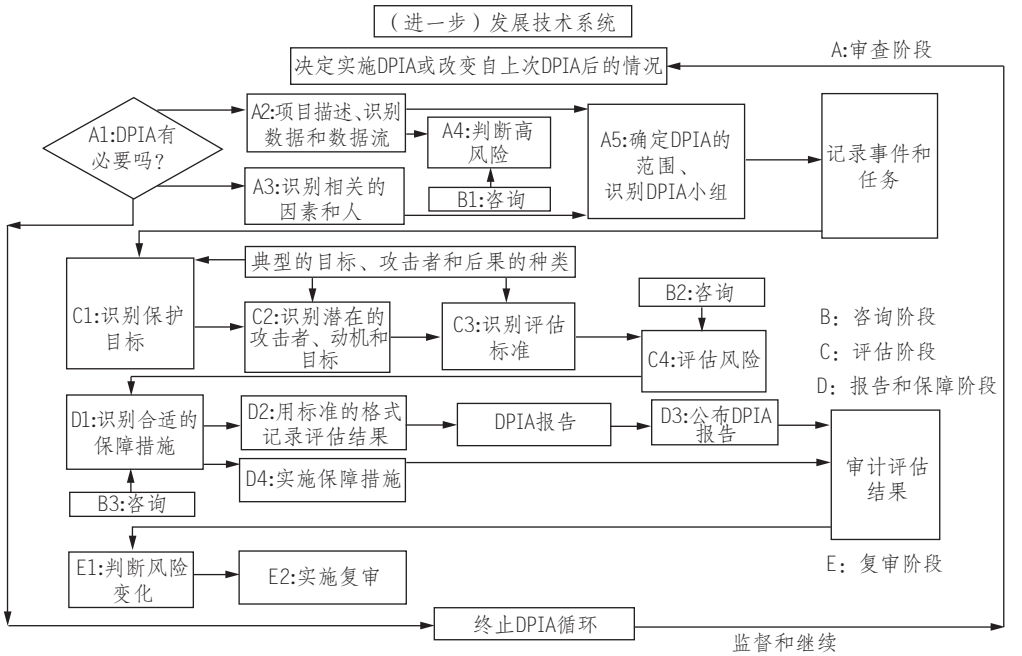

图 3　DPIA 具体流程

3.1　审查阶段

审查是 DPIA 的第一个步骤,其任务是对所涉数据处理行为进行初步的分析,判断是否需要实施 DPIA,整个阶段需要记录。实施 DPIA 的前提是,数据处理行为可能会对自然人的权利和自由产生高风险,即审查数据处理行为是否运用了新技术,或是分析其是否符合自动化系统处理和评估个人信息、大规模处理特殊数据、大规模系统监测公开访问区域这三种情形。《12 草案》规定的情形是“数据处理行为可能会对数据主体的权利和自由产生特殊风险时”,GDPR 规定的是“当一种数据处理行为运用新技术可能会对自然人的权利和自由产生高风险时”,这样的修改体现了 DPIA 制度的选择性和保护个人数据的核心。数据处理行为通常以项目或计划等形式呈现,审查阶段需要收集关于目标项目或计划的所有基本资料,对项目或计划的主要内容、所涉技术和利益相关者进行分析,从而获知项目或计划的影响范围和影响因素。通过咨询判断是否具有高风险,如果有,则根据审查和咨询的结果确定 DPIA 制度的目标和范围并形成 DPIA 小组,否则将直接进行目标数据处理。

3.2　咨询阶段

咨询是穿插在审查、评估、报告和保障阶段之中的,内容涉及三个环节、三个对象。咨询的对象不仅包括利益相关者,还包括数据保护的专门人员和机构。利益相关者主要是数据主体或其代表人以及相关的公司或组织,数据保护的专门人员和机构指数据保护官和数据保护监管机构。首先在判断是否具有高风险的环节中,数据控制者需要根据 DPIA 范围的指向性以及利益相关者的基本情况分析制定咨询策略,咨询数据主体和各利益相关者。同时,可以向数据保护官寻求建议(在数据控制者指定了数据保护官的情况下应当咨询数据保护官)。在评估风险等级时,如果已经识别出数据处理将会给自然人的权利和自由带来高风险,或是数据控制者认为根据现有的技术和实施成本所采

取的合理手段不能减少风险,则都应在数据处理活动之前咨询监管机构。监管机构应在规定期限内对咨询请求做出回应,其可根据本条例规定做出临时或永久禁止数据处理行为的决定。最后在确定保障措施的环节中,数据控制者应当咨询数据主体或其代表人以及利益相关者,以确保安全保障措施能够在尽量不损害商业利益的情况下最大限度保护个人数据。

3.3 评估阶段

实施 DPIA 的工作人员必须具备相应的专业能力以进行客观地评估,应当有一个中立的组织协助评估以保证质量。首先要根据审查阶段所获取的基本信息确定保护的目标,通过对项目或计划的"模拟演练",识别潜在的攻击者、攻击者的动机和攻击后果的种类,进而识别评估标准。保护的目标包括可得性、完整性、保密性、不可链接性、透明性和不可干涉性。每一个目标都不容忽视,对目标的忽视即视为对数据主体权利的侵害从而构成实施 DPIA 制度的"风险"。但是各目标之间存在着一定的矛盾,比如可得性和保密性,因而要注意目标之间的平衡[11]。其次,确定评估项目或计划的风险等级,等级包括正常、高、非常高。"正常"是指处理个人数据时没有任何场景表明处理的性质显示有高强度干扰的可能性。"高"是指当数据处理会严重干扰有关人员,且缺乏有效的保障措施和干预手段,处理数据需要法律的高保护标准或取决于公司决策者。"非常高"是指是否需要高保护标准的个人数据处理取决于本公司的决定或有关人员,而且,有关人员不能意识到,也难以自己纠正由于数据安全性不足或处理目的的非法改变而造成额外风险。评估结果需要中立、客观的组织进行审计。

3.4 报告和保障阶段

在评估之后,数据控制者需要用特殊格式制作并公布 DPIA 报告,报告可以作为相关的证据使用。每个公司或组织收集每次的 DPIA 报告形成"公司记忆库"(Corporate Memory),以保证所获取的经验以后还能够反复适用[4]。且 GDPR 在《12 草案》的基础之上增加了"一个评估可能解决一系列具有相同高风险的类似数据处理操作"的规定,类似情况类似处理的方法使得企业的适用成本大幅减少。针对评估的不同等级,数据控制者有控制(Treat)、接受(Tolerate)、终止(Terminate)和转移(Transfer)四种回应方式,可单独采用,也可组合采用。"控制"包括调整(Risk Modifiacation),适用于控制后风险能降至可接受范围的情形。"接受"含容忍之意,适用于风险极小、控制风险成本远远大于商业利益的情形。"终止"的目的在于避免风险(Risk Avoidance),适用于风险高、控制风险成本过多、投资回报过少的情形。"转移"指分享风险(Risk Sharing),适用于风险高、控制风险成本多、但项目非常有价值的情形(见表 1)[13]。

表 1 数据控制者的回应方式

方式	内容	适用情形
Treat	控制、调整	控制后,风险能降至可接受范围
Tolerate	容忍、接受	风险极小,控制风险成本远远大于商业利益
Terminate	避免、终止	风险高,控制风险成本过多,投资回报过少
Transfer	分享、转移	风险高,控制风险成本多,但项目太有价值

3.5 复审阶段

复审也是 GDPR 新增的内容,指报告完成之后数据控制者在必要时应当核实数据处理是否按照评估结果采取了相应的保障措施,实际操作中复审还有可能引发 DPIA 的再次实施。必要时是指在数据处理风险产生变化时,即指

公司或法律条件发生变化或识别出数据保护普遍存在的新风险,且必须确保所选择的保障措施能够适应这些变化。复审的目的在于持续监测,DPIA 不是一个单一的、线性的过程,要反复实施以保证项目整个生命周期的持续监督。

4　欧盟 DPIA 制度对我国的启示

大数据的出现使得信息收集和保存方法发生了改变。在中国,我们不难发现大街小巷随处可见的摄像头,互联网上各种各样的监控软件,甚至随身携带的手机都在时时刻刻对我们个人数据进行着自动记录。“中国不是信息化起始早的国家,但是一个发展尤为迅速的国家。”[14]在这样一个国度,我们更需采取措施积极应对洪水猛兽般的数据安全问题。DPIA 制度通过对数据控制者的义务设定和周密的流程设计,强化了对数据风险的事前防控,这样的制度安排一方面有助于相关企业节约成本、赢得消费者信任和市场美誉,另一方面也有利于数据主体实现对自身数据的掌控和保护。

4.1　对我国选择数据保护影响评估立法模式的启示

从欧盟的 PIA 制度到 DPIA 制度的演进路径及其发展模式来看,我国在数据保护影响评估的立法模式上有两种选择,一是由国家出台指导性规范,在此基础上积极推进行业自律;二是将数据保护影响评估设置成一项强制性义务。当然,模式选择取决于大数据技术应用渗透深度、数据产业发展速度以及社会发展阶段等诸多因素,在大数据发展初期,前一种模式是一个更优的选项,但在大数据产业发展到一定阶段之后,后一种模式也许更符合社会发展的需要。

(1)选择指导性规范与行业自律结合模式

Finn 和 Wright 认为,数据问题在很大程度上是一个道德问题[15]。Mantelero 认为,面对硬性法律规范,企业更愿意支持系统的自我调节,采用行业自律与国家标准相结合的模式,能够确保所有利益相关者的参与[16]。只有通过企业自主地发现问题、解决问题才会形成根深蒂固的影响。将 DPIA 设置成一项强制性义务,考虑到当前中国尚未建构好基本的数据保护法律体系,这种模式需要大量的立法、司法和执法成本,因而不是当前的优选项。相反,我国应积极发挥行业自律的作用,市场能够解决的由市场解决,辅之以政策推动,不失为当前的一种更理想的选择。由国家或各省市出台相关的指导性鼓励规范,各企业可将 DPIA 制度纳入公司章程以及公司管理制度之中,并参照国家指导性规范在各企业内部进行管理。数据主体只需和相关企业联系,不必花费过多的时间、金钱。

(2)选择强制性义务模式

随着大数据技术的快速发展和深入渗透,数据保护影响评估的社会需求将日益迫切。虽然指导性规范与行业自律相结合模式的成本低,但无强制则无保障,采用这种模式可能导致自然人的权益处于高风险之中[17]。企业为节约成本很可能不实施 DPIA,或是为了获取消费者信任,只采取了形式上的 DPIA 或是选择性地采取 DPIA 的部分程序,从而未能实质性地有效保护数据主体的权利,且权力主体(监管机构)和责任规制的缺失将会直接影响数据主体的权益救济。因此,我国有必要在条件成熟的时候,根据现实需要实现立法模式的转换,在数据产业高速发展、个人数据安全面临更大风险的时候,把 DPIA 设置为数据控制者的一项强制性义务,也许只有这样才能达到数据保护风险的事前防控效果。这在我国是可行的,原因有二:

首先,从立法技术上来看,中欧都是大陆法系,至少在法治土壤的大背景之下不具明显冲突。我国现有立法中不乏与 DPIA 制度相类似的风险防范机制,典型的例子有近几年才制定的环境保护影响评估和食品安全风险评估。风险防范机制从本质上来说都是相似的,DPIA 制度只是在数据保护范围内的一项风险防范机制而已。数据处理中数据主体遭遇的风险并不比

环境保护和食品安全管理的风险低,就现今环境保护影响评估和食品安全风险评估的实施和效果来看,可以说将 DPIA 制度设为一项强制性义务在中国的立法技术上是完全可行的。

其次,从 DPIA 这项制度的义务主体——相关企业来看,虽然增设 DPIA 这一项强制性义务将导致其需要承担较高的成本,因为进行数据保护影响评估就必然需要投入必要的人力和财力,但是从最终的结果来看,增设这样一项义务对企业将起到"正和"而非"零和"的作用。其原因在于:第一,大数据时代,企业通过数据保护影响评估,事实上是为保护消费者数据、有效控制数据处理的风险提供必要的机制保障,防患于未然,这样往往更能赢得消费者的信任。消费者是企业运营要考虑的首要因素,企业提供的产品、服务能否取得消费者的信赖,直接决定了企业的成败。第二,DPIA 这样的制度安排在大数据时代无疑也是一种兼顾安全和效率的平衡机制。给高速运转的企业装上数据安全阀,在数据利用乱象丛生的当代社会,已经显得日益迫切。根据经济学中"商业成本内部化"的理论,不能只着眼于前期投入而忽视后期回报,安全的高品质产品和服务必然带来高价格,消费者想要获取理想的产品和服务毫无疑问需要付出相应的代价。最终企业获得的回报是"高代价+高信赖+利润",这将远远超过前期投入。

4.2 对我国制定信息(数据)保护影响评估的具体规定的启示

目前,我国与欧盟 DPIA 相对应的规定主要体现在《网络安全法》和《信息安全技术个人信息安全规范》(简称《规范》)中。《网络安全法》中的相关规定非常粗略,仅规定了国家鼓励各单位进行风险评估,针对关键信息基础设施运营者需个人信息和重要数据出境时应当进行评估,其他情形时每年至少一次评估(其具体的配套规定《个人信息和重要数据出境安全评估办法》《信息安全技术数据出境安全评估指南》都还在征求意见阶段)。所以,目前我国关于信息(数据)保护影响评估的具体规定主要体现在《规范》之中。

全国信息安全标准化技术委员会于 2016 年 12 月发布了《规范》(征求意见稿),于 2017 年 11 月 30 日发布《规范》(报批稿),2017 年 12 月 29 日该规范正式通过,2018 年 5 月 1 日开始实施。全国信息安全标准化技术委员会采用推荐性国家标准的形式,为规范个人信息控制者的信息处理、保障个人信息的安全制定此《规范》。最后通过的版本较征求意见稿而言,在内容编排上只进行了细微的调整,而对于内容的分布有较大改变。有关个人信息安全影响评估的内容大幅删减,相反,关于隐私政策的规范大幅增加。最后通过的版本完全删除了对个人信息安全影响评估的流程解释,并对征求意见稿中的一些相关规范也作了修改。

在该《规范》中,个人信息安全影响评估被定义为"针对个人信息处理活动,检验其合法合规程度,判断其对个人信息主体合法权益造成损害的各种风险,以及评估用于保护个人信息主体的各项措施有效性的过程"[18]。实施主体是个人信息控制者,规制对象是个人信息处理活动,流程分为分析、评估、报告与保障、跟踪四个阶段。首先,针对个人信息控制者的个人信息处理过程进行全面的调研,区分个人敏感信息和普通个人信息的边界,梳理个人信息处理活动的类型,研究所采取的安全措施,从而判断个人信息处理活动是否会对个人信息主体权益产生风险。然后,依照审批稿规定的评估内容,从个人信息处理活动和安全事件的风险程度与可能性两个要素出发评定风险等级。之后根据相应等级给出相关改进建议,形成影响评估报告并以适宜的形式对外公开。最后,在法律法规有新的要求时,或在业务模式、信息系统、运行环境发生重大变更时,或发生个人信息安全事件时,应重新进行个人信息安全影响评估[19]。

最后通过的版本不仅删除了征求意见稿中评估流程方面的内容,还对一些重要的条款作了修改和删除。就评估的内容而言,删除了"变更

处理目的对个人信息主体合法权益可能产生的影响”这一要求/内容,显然违背了个人信息安全原则中的“目的明确原则”①和“最少够用原则”②。删除了对重大变更以及个人信息安全事件的列举,而最后版本中对此也无相关定义,这使得“重新进行个人信息安全影响评估的情形”难以确定。特定情况下,个人信息控制者要设立专职的个人信息保护负责人和个人信息保护工作机构,这些负责人和工作机构的职责之一就是开展个人信息安全影响评估,删除“个人信息安全执行责任人或个人信息安全专员,应审核个人信息影响评估报告”,这一步骤实属合理。然而,删除“风险无法接受则应及时停止执行”的规定,将“个人信息安全影响评估报告定期对外公布”修改成“以适宜的形式对外公开”,会加大个人信息的安全风险。删除“可以选择外部机构进行影响评估”的规定,则代表个人信息控制者只能内部自行评估,更有利于贯彻权责一致原则③。

此外,该《规范》对于“信息”和“数据”未做明确区分。其中关于“个人信息控制者”“个人信息主体”“个人信息”的概念分别与欧盟“数据控制者”“数据主体”“个人数据”的含义一致。虽然采用的是“信息”这一概念,相对应的英文是“Information”,但是在“个人信息主体”和“个人信息控制者”定义时却以“Data”取代了“Information”。

相比于欧盟的 DPIA 制度,我国《规范》在数据保护影响评估流程设计上缺乏咨询阶段,复审阶段在我国的安全评估中未体现充分的重要性。《规范》的性质定位为推荐性国家标准,并非强制性国家标准。从现实情况来看,还存在监管主体缺位的问题,上述多个原因将使得整个评估实施的效果必然会相差甚远。此外,DPIA 的适用情形是对个人的权利和自由会产生高风险的情形,其范围明显大于我国的个人信息安全评估的范围。而这几个方面的差异正是我国信息(数据)保护影响评估制度需要重点补充和完善的部分。

5　结语

综上所述,DPIA 制度流程上分为审查、咨询、评估、报告和保障以及复审五个阶段,其对数据保护风险事前防范的强调以及服务于风险全面防范的审慎的具体流程的设计,可以实现把控风险、保护个人数据安全的双重目的,同时有助于企业节约成本、赢得消费者信任。欧盟 DPIA 制度对我国完善个人信息(数据)保护影响评估制度有着重要的借鉴意义,我国应着重完善在评估流程设计、评估性质和监管主体建设等方面的具体规定。

参考文献

[1] European Comission. EU data protection reform what benefits for businesses in Europe? [EB/OL].[2018-02-15].http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=52404.

[2] 迪莉娅. 大数据环境下隐私泄露影响评估研究[J]. 情报杂志,2016,35(4):141-146.(Di Liya. Studies on privacy impact assessment in the big data environment[J]. Journal of Intelligence, 2016,35(4):141-146.)

[3] European Comission. Privacy and data protection impact assessment framework for RFID applications[EB/OL].[2018-02-15].http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp180_annex_en.pdf.

① 目的明确原则指具有合法、正当、必要、明确的个人信息处理目的。

② 最少够用原则指除与个人信息主体另有约定外,只处理满足个人信息主体授权同意的目的所需的最少个人信息类型和数量。目的达成后,应及时根据约定删除个人信息。

③ 权责一致原则指对其个人信息处理活动对个人信息主体合法权益造成的损害承担责任。

[4] Wright D. The state of the art in privacy impact assessment[J]. Computer Law & Security Review, 2012, 28(1): 54-61.

[5] Wright D. Making privacy impact assessment more effective[J]. The Information Society, 2013, 29(5): 307-315.

[6] Warren A, Bayley R, Bennett C, et al. Privacy impact assessments: international experience as a basis for UK guidance[J]. Computer Law & Security Review, 2008, 24(3):233-242.

[7] Wright D, Raab C. Privacy principles, risks and harms[J]. International Review of Law, Computers & Technology, 2014, 28(3): 277-298.

[8] Kuner C. 欧洲数据保护法[M].旷野,杨会永,译. 北京:法律出版社, 2008:79.(Kuner C. European Data Protection Law[M]. Kuang Ye, Yang Huiyong,trans. Beijing: Law Press, 2008:79.)

[9] Quelle C. The 'risk revolution' in *EU data protection law*: we can't have our cake and eat it, too[J]. Social Science Electronic Publishing, 2017.

[10] 高富平.个人数据保护和利用国际规则源流与趋势[M].北京:法律出版社,2016:245.(Gao Fuping. International rules on personal data protection and use: origin and trend[M].Beijing: Law Press , 2016:245.)

[11] Data protection-Better rules for small business[EB/OL].[2018-02-15]. http://ec.europa.eu/justice/newsroom/data protection/infographic/2017/index_en.htm.

[12] Bieker F, Friedewald M, Hansen M, et al. A process for data protection impact assessment under the European general data protection regulation[C]// Privacy Forum. Springer International Publishing, 2016:21-37.

[13] IT GOVERNANCE PRIVACY TEAM. EU general data protection regulation (GDPR): an implementation and compliance guide[M].Ely, Cambridgeshire, United Kingdom: IT Governance Publishing,2017:130-131.

[14] 郭瑜.个人数据保护法研究[M].北京:北京大学出版社,2012.(Guo Yu. Legal protection of personal data[M]. Beijing: Peking University Press, 2012.)

[15] Finn R L, Wright D. Privacy, data protection and ethics for civil drone practice: a survey of industry, regulators and civil society organizations[J]. Computer Law & Security Review, 2016, 32(4):577-586.

[16] Mantelero A. The privacy impact assessment in the EU proposal of general regulation on data protection[J]. Social Science Electronic Publishing, 2012(1):145-153.

[17] Binns R. Data protection impact assessments: a meta-regulatory approach [J/OL].[2018-02-18](2016-12-13). International Data Privacy Law, 2017, 7(1): 22-35. https://ssrn.com/abstract=2964242.

[18] 国家标准化管理委员会.信息安全技术个人信息安全规范[EB/OL].[2018-02-18].http://www.sohu.com/a/220032846_353595.(Standardization Administration of the People's Republic of China. Information security technology-personal information security specification [EB/OL].[2018-02-18].http://www.sohu.com/a/220032846_353595.)

[19] 国家标准化管理委员会.信息安全技术个人信息安全规范(征求意见稿)[EB/OL].[2018-02-18]. http://politics.gmw.cn/2016-09/20/content_22064789.htm.(Standardization Administration of the People's Republic of China. Information security technology-personal information security specification(Draft)[EB/OL].[2018-02-18].http://politics.gmw.cn/2016-09/20/content_22064789.htm.)

肖冬梅 湘潭大学法学院教授。湖南 湘潭 411105。

谭礼格 湘潭大学法学院2016级硕士研究生。湖南 湘潭 411105。

(收稿日期:2018-06-08)